UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/928,133	08/10/2001	Russell Andrew Fink	00-4045	6468

32127 7590 10/14/2005

VERIZON CORPORATE SERVICES GROUP INC.
C/O CHRISTIAN R. ANDERSEN
600 HIDDEN RIDGE DRIVE
MAILCODE HQE03H14
IRVING, TX 75038

EXAMINER	
TESLOVICH, TAMARA	
ART UNIT	**PAPER NUMBER**
2137	

DATE MAILED: 10/14/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/928,133	FINK ET AL.	
	Examiner	Art Unit	
	Tamara Teslovich	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 July 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-24* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-24* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

The amendment filed July 7, 2005 is objected to under 35 U.S.C. 132(a) because it introduces new matter into the disclosure. 35 U.S.C. 132(a) states that no amendment shall introduce new matter into the disclosure of the invention. The added material which is not supported by the original disclosure is as follows: "a host resolution device adapted to determine the addresses of devices on the network when the address does not match an entry in the host table, and to supplement the host table with any additional addresses." The Applicant has added the abovementioned feature to each of the independent claims 1, 6, 11, and 16. Independent claims 4, 9, 14, and 19 rely on the added material of claims 1, 6, 11, and 16 respectively and are objected to accordingly. Applicant is required to cancel the new matter in the reply to this Office Action.

In reference to newly added claims 21-24, the Examiner has agreed to allow the new claims. The rejection of each of the newly added claims appears below.

The Examiner would like to make note that the Applicant has not argued any of the Examiner's 102 or 103 rejections from the previous office action, which the Examiner has taken as a sign of agreement by the Applicant in regards to the Examiner's previous rejections.

Therefore, based on the above arguments, the Examiner maintains the rejections as set forth below.

Claim Rejections - 35 USC § 102

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claims 1-24 are rejected under 35 U.S.C. 102(b) as being anticipated by Kraemer et al. (U.S. Patent No. 5,798,706).

As per Claim 1, Kraemer et al. discloses an apparatus for detecting adversarial activity on a network, comprising a memory adapted to store a host table (see col.3 lines 46-60); a key exchanger adapted to derive a cipher key (see page 2 of WIPO Publication No. 97/26734 -- incorporated by Kraemer et al. in col.3 lines 40-45, reference "VPN"); a translator adapted to translate predetermined portions of packet header information of a data packet according to a cipher algorithm keyed by the cipher key (see page 2 of WIPO Publication No. 97/26734 -- incorporated by Kraemer et al. in col.3 lines 40-45, reference "VPN"), wherein the predetermined portions include an address (see col.4 lines 33-46); a mapping device adapted to map the address to the host table (see col.3 line 60 thru col.4 line 2); and an actuator adapted to trigger a security device when the address does not match an entry in the host table (see col.4 lines 3-5 and 20-32).

As per Claim 2, Kraemer et al. discloses an apparatus as set forth in Claim 1, wherein the security device is a logging device adapted to log the data packet (see col.4 lines 3-5 and 26-31).

As per Claim 3, Kraemer et al. discloses an apparatus as set forth in Claim 1, wherein the security device is adapted to signal an alarm when triggered (see col.2 lines 27-31 and col.4 lines 20-25).

As per Claim 4, Kraemer et al. discloses an apparatus as set forth in Claim 1, further comprising a host resolution device adapted to derive the host table using an address resolution protocol (see col.4 lines 48-52).

As per Claim 5, Kraemer et al. discloses an apparatus as set forth in Claim 1, further comprising a network device adapted to place the data packet onto a network when the address maps to the host table (col.1 line 66 through col.2 line 9 and col.2 lines 27-31).

As per Claim 6, Kraemer et al. discloses a method for detecting adversarial activity on network, comprising storing a host table (see col.3 lines 46-60); deriving a cipher key (see page 2 of WIPO Publication No. 97/26734 -- incorporated by Kraemer et al. in col.3 lines 40-45, reference "VPN"); translating predetermined portions of packet header information of a data packet according to a cipher algorithm keyed by the cipher key (see page 2 of WIPO Publication No. 97/26734 -- incorporated by Kraemer et al. in col.3 lines 40-45, reference "VPN"), wherein the predetermined portions include an address (see col.4 lines 33-46); mapping the address the host table (see col.3 line 60 thru col.4 line 2); and triggering a security device when the address does not match an entry in the host table (see col.4 lines 3-5 and 20-32).

As per Claim 7, Kraemer et al. discloses a method as set forth in Claim 6, further comprising logging the data packet when the address does not match an entry in the host table (see col.4 lines 3-5 and 26-31).

As per Claim 8, Kraemer et al. discloses a method as set forth in Claim 6, further comprising signaling an alarm when the security device is triggered (see col.2 lines 27-31 and col.4 lines 20-25).

As per Claim 9, Kraemer et al. discloses a method as set forth in Claim 6, further comprising deriving the host table using an address resolution protocol (see col.4 lines 48-52).

As per Claim 10, Kraemer et al. discloses a method as set forth in Claim 6, further comprising placing the data packet onto a network when the address maps to the host table (see col.4 lines 3-5 and 26-31).

As per Claim 11, Kraemer et al. discloses a device for detecting adversarial activity on a network, comprising means for storing a host table (see col.3 lines 46-60); means for deriving a cipher key (see page 2 of WIPO Publication No. 97/26734 -- incorporated by Kraemer et al. in col.3 lines 40-45, reference "VPN"); means for translating predetermined portions of header information of a data packet according to a packet cipher algorithm keyed by the cipher key (see page 2 of WIPO Publication No. 97/26734 -- incorporated by Kraemer et al. in col.3 lines 40-45, reference "VPN"), wherein the predetermined portions include an address (see col.4 lines 33-46); means for mapping the address to the host table (see col.3 line 60 thru col.4 line 2); and means

for triggering a security device when the address does not match an entry in the host table (see col.4 lines 3-5 and 20-32).

As per Claim 12, Kraemer et al. discloses a device as set forth in Claim 11, further comprising means for logging the data packet when the address does not match an entry in the host table (see col.4 lines 3-5 and 26-31).

As per Claim 13, Kraemer et al. discloses a device as set forth in Claim 11, further comprising means for signaling an alarm when the security device is triggered (see col.2 lines 27-31 and col.4 lines 20-25).

As per Claim 14, Kraemer et al. discloses a device as set forth in Claim 11, further comprising means for deriving the host table using an address resolution protocol (see col.4 lines 48-52).

As per Claim 15, Kraemer et al. discloses a device as set forth in Claim 11, further comprising means for placing the data packet network when the address maps to the host table (see col.4 lines 3-5 and 26-31).

As per Claim 16, Kramer et al. discloses a bastion host adapted for processing packet header information of a data packet, the bastion host being operable to store a host table (see col.3 lines 46-60) derive a cipher key (see page 2 of WIPO Publication No. 97/26734 -- incorporated by Kraemer et al. in col.3 lines 40-45, reference "VPN"); translate predetermined portions of packet header information of a data packet according to a cipher algorithm keyed by the cipher key (see page 2 of WIPO Publication No. 97/26734 -- incorporated by Kraemer et al. in col.3 lines 40-45,

reference"VPN"), wherein the predetermined portions include an address (see col.4 lines 33-46); map the address to the host table (see col.3 line 60 thru col.4 line 2); and trigger a security device when the address does not match an entry in the host table (see col.4 lines 3-5 and 20-32).

As per Claim 17, Kraemer et al. discloses the bastion host as set forth in Claim 16, the bastion host being further operable to log the data packet when the address does not match an entry in the host table (see col.4 lines 3-5 and 26-31).

As per Claim 18, Kraemer et al. discloses the bastion host as set forth in Claim 16, the bastion host being further operable to signal an alarm when the security device is triggered (see col.2 lines 27-31 and col.4 lines 20-25).

As per Claim 19, Kraemer et al. discloses the bastion host as set forth in Claim 16, the bastion host being further operable to deriving the host table using an address resolution protocol (see col.4 lines 48-52).

As per Claim 20, Kraemer et al. discloses the bastion host as set forth in Claim 16, the bastion host being further operable to place the data packet onto a network when the address maps to the host table (see col.4 lines 3-5 and 26-31).

As per Claim 21, Kraemer et al. discloses the apparatus as set forth in Claim 1, wherein said key exchanger is further adapted to repeatedly derive a cipher key with the cipher key derived by said key exchanger over time (see page 8 lines 10-15, and page 11 line 31 thru page 13 line 5 of WIPO Publication No. 97/26734 -- incorporated by Kraemer et al. in col.3 lines 40-45, reference "VPN").

As per Claim 22, Kraemer et al. discloses the method as set forth in Claim 6, wherein deriving the cipher key comprises repeatedly deriving a cipher key such that the resulting cipher key changes over time (see page 8 lines 10-15, and page 11 line 31 thru page 13 line 5 of WIPO Publication No. 97/26734 -- incorporated by Kraemer et al. in col.3 lines 40-45, reference "VPN").

As per Claim 23, Kraemer et al. discloses the device as set forth in Claim 11, wherein said means for deriving a cipher key is further adapted to repeatedly derive a cipher key such that the resulting cipher key changes over time (see page 8 lines 10-15, and page 11 line 31 thru page 13 line 5 of WIPO Publication No. 97/26734 -- incorporated by Kraemer et al. in col.3 lines 40-45, reference "VPN").

As per Claim 24, Kraemer et al. discloses the bastion host as set forth in Claim 16, wherein said the bastion host is further operable to repeatedly derive a cipher key such that the resulting cipher key changes over time (see page 8 lines 10-15, and page 11 line 31 thru page 13 line 5 of WIPO Publication No. 97/26734 -- incorporated by Kraemer et al. in col.3 lines 40-45, reference "VPN").

Claims 1-3, 5-8, 10-13, 15-18, and 2-24 are rejected under 35 U.S.C. 102(b) as being anticipated by Deng et al. (U.S. Patent No. 6,701,432 B1).

As per Claim 1, Deng et al. discloses an apparatus for detecting adversarial activity on a network, comprising a memory adapted to store a host table (see col.5 line 61 thru col.6 line 23 and col.9 lines 1-20); a key exchanger adapted to derive a cipher

key (see col.10 lines 13-51); a translator adapted to translate predetermined portions of packet header information of a data packet according to a cipher algorithm keyed by the cipher key, wherein the predetermined portions include an address (see col.10 lines 13-51); a mapping device adapted to map the address to the host table (see col.6 lines 16-48 and col.7 lines 1-5); and an actuator adapted to trigger a security device when the address does not match an entry in the host table (see col.9 lines 45-49).

As per Claim 2, Deng et al. discloses an apparatus as set forth in Claim 1, wherein the security device is a logging device adapted to log the data packet (see col.9 lines 45-49).

As per Claim 3, Deng et al. discloses an apparatus as set forth in Claim 1, wherein the security device is adapted to signal an alarm when triggered (see col.9 lines 45-49).

As per Claim 5, Deng et al. discloses an apparatus as set forth in Claim 1, further comprising a network device adapted to place the data packet onto a network when the address maps to the host table (col.9 lines 50-57).

As per Claim 6, Deng et al. discloses a method for detecting adversarial activity on network, comprising storing a host table (see col.5 line 61 thru col.6 line 23 and col.9 lines 1-20); deriving a cipher key (see col.10 lines 13-51); translating predetermined portions of packet header information of a data packet according to a cipher algorithm keyed by the cipher key, wherein the predetermined portions include an address (see col.10 lines 13-51); mapping the address the host table (see col.6 lines 16-48 and col.7

lines 1-5); and triggering a security device when the address does not match an entry in the host table (see col.9 lines 45-49).

As per Claim 7, Deng et al. discloses a method as set forth in Claim 6, further comprising logging the data packet when the address does not match an entry in the host table (see col.9 lines 45-49).

As per Claim 8, Deng et al. discloses a method as set forth in Claim 6, further comprising signaling an alarm when the security device is triggered (see col.9 lines 45-49).

As per Claim 10, Deng et al. discloses a method as set forth in Claim 6, further comprising placing the data packet onto a network when the address maps to the host table (col.9 lines 50-57).

As per Claim 11, Deng et al. discloses a device for detecting adversarial activity on a network, comprising means for storing a host table (see col.5 line 61 thru col.6 line 23 and col.9 lines 1-20); means for deriving a cipher key (see col.10 lines 13-51); means for translating predetermined portions of header information of a data packet according to a packet cipher algorithm keyed by the cipher key, wherein the predetermined portions include an address (see col.10 lines 13-51); means for mapping the address to the host table (see col.6 lines 16-48 and col.7 lines 1-5); and means for triggering a security device when the address does not match an entry in the host table (see col.9 lines 45-49).

As per Claim 12, Deng et al. discloses a device as set forth in Claim 11, further comprising means for logging the data packet when the address does not match an entry in the host table (see col.9 lines 45-49).

As per Claim 13, Deng et al. discloses a device as set forth in Claim 11, further comprising means for signaling an alarm when the security device is triggered (see col.9 lines 45-49).

As per Claim 15, Deng et al. discloses a device as set forth in Claim 11, further comprising means for placing the data packet network when the address maps to the host table (col.9 lines 50-57).

As per Claim 16, Deng et al. discloses a bastion host adapted for processing packet header information of a data packet, the bastion host being operable to store a host table (see col.5 line 61 thru col.6 line 23 and col.9 lines 1-20); derive a cipher key (see col.10 lines 13-51); translate predetermined portions of packet header information of a data packet according to a cipher algorithm keyed by the cipher key, wherein the predetermined portions include an address portions include an address (see col.10 lines 13-51); map the address to the host table (see col.6 lines 16-48 and col.7 lines 1-5); and trigger a security device when the address does not match an entry in the host table (see col.9 lines 45-49).

As per Claim 17, Deng et al. discloses the bastion host as set forth in Claim 16, the bastion host being further operable to log the data packet when the address does not match an entry in the host table (see col.9 lines 45-49).

As per Claim 18, Deng et al. discloses the bastion host as set forth in Claim 16, the bastion host being further operable to signal an alarm when the security device is triggered (see col.9 lines 45-49).

As per Claim 20, Deng et al. discloses the bastion host as set forth in Claim 16, the bastion host being further operable to place the data packet onto a network when the address maps to the host table (col.9 lines 50-57).

As per Claim 21, Dent et al. discloses the apparatus as set forth in Claim 1, wherein said key exchanges is further adapted to repeatedly derive a cipher key with the cipher key derived by said key exchanger changing over time (col.5 lines 38-55 reference "DES").

As per Claim 22, Dent et al. discloses the method as set forth in Claim 6, wherein deriving the cipher key comprises repeatedly deriving a cipher key such that the resulting cipher key changes over time (col.5 lines 38-55 reference "DES").

As per Claim 23, Dent et al. discloses the device as set forth in Claim 11, wherein said means for deriving a cipher key is further adapted to repeatedly derive a cipher key such that the resulting cipher key changes over time (col.5 lines 38-55 reference "DES").

As per Claim 24, Dent et al. discloses the bastion host as set forth in Claim 16, wherein the bastion host is further operable to repeatedly derive a cipher key such that the resulting cipher key changes over time (col.5 lines 38-55 reference "DES").

Claim Rejections - 35 USC § 103

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claims 4, 9, 14, and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Deng as applied to claims 1, 6, 11, and 16 above, and further in view of Kraemer et al. (U.S. Patent No. 5,798,706).

As per Claim 4, Deng et al. discloses an apparatus as set forth in Claim 1, but fails to disclose a host resolution device adapted to derive the host table using an address resolution protocol.

Kraemer et al. discloses a host resolution device adapted to derive the host table using an address resolution protocol (see col.4 lines 48-52).

It would have been obvious to a person of average skill in the area at the time of the invention to include within Deng's apparatus for detecting adversarial activity on a network Kraemer's ARP derived host table in order that an administrator without knowledge of the hardware addresses of the devices connected to the network, need not be burdened with entering by hand the MAC addresses of each device.

As per Claim 9, Deng et al. discloses a method as set forth in Claim 6, but fails to disclose deriving the host table using an address resolution protocol.

Kraemer et al. discloses deriving the host table using an address resolution protocol (see col.4 lines 48-52).

It would have been obvious to a person of average skill in the area at the time of the invention to include within Deng's apparatus for detecting adversarial activity on a network Kraemer's ARP derived host table in order that an administrator without knowledge of the hardware addresses of the devices connected to the network, need not be burdened with entering by hand the MAC addresses of each device.

As per Claim 14, Deng et al. discloses a device as set forth in Claim 11, but fails to disclose means for deriving the host table using an address resolution protocol.

Kraemer et al. discloses deriving the host table using an address resolution protocol (see col.4 lines 48-52).

It would have been obvious to a person of average skill in the area at the time of the invention to include within Deng's apparatus for detecting adversarial activity on a network Kraemer's ARP derived host table in order that an administrator without knowledge of the hardware addresses of the devices connected to the network, need not be burdened with entering by hand the MAC addresses of each device.

As per Claim 19, Deng et al. discloses the bastion host as set forth in Claim 16, but fails to disclose the bastion host being further operable to deriving the host table using an address resolution protocol.

Kraemer et al. discloses the bastion host being further operable to deriving the host table using an address resolution protocol (see col.4 lines 48-52).

It would have been obvious to a person of average skill in the area at the time of the invention to include within Deng's apparatus for detecting adversarial activity on a network Kraemer's ARP derived host table in order that an administrator without knowledge of the hardware addresses of the devices connected to the network, need not be burdened with entering by hand the MAC addresses of each device.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tamara Teslovich whose telephone number is (571) 272-4241. The examiner can normally be reached on Mon-Fri 8-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

T. Teslovich
October 10, 2005

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER